Attacks on Sensing in Hostile Wireless Sensor-Actuator Environments

Alexandra Czarlinska
Department of ECE
Texas A&M University,
College Station, Texas 77843
Email: czlinska@ece.tamu.edu

William Luh
Department of ECE
Texas A&M University,
College Station, Texas 77843
Email: luh@ece.tamu.edu

Deepa Kundur
Department of ECE
Texas A&M University,
College Station, Texas 77843
Email: deepa@ece.tamu.edu

***Abstract*—Wireless Sensor Networks (WSNs) deployed in hostile environments are susceptible to various attacks directed at their data. In this work we focus on an emerging and largely unexplored issue arising from the presence of actuator (or actor) nodes in the form of Wireless Sensor Actuator Networks (WSANs). Specifically, we consider the case where hostile WSAN nodes belonging to a foreign network directly perturb the readings of WSN nodes during sensing. The attack is modeled as affecting the decision that a WSN node reports about the presence or absence of a phenomenon to its cluster head. To assess the potential loss of sensing fidelity due to the opposing network, we employ a game theoretic analysis. We focus on determining the probability that the WSN cluster head becomes alerted to such an attack given some statistical information about the phenomenon. Our results show that an actuation attack may go unnoticed even if such an attack is not coordinated among the hostile WSAN nodes. Importantly, the number of WSN nodes in a cluster affects the probability of WSAN attack success. For clusters consisting of only a few nodes, the hostile WSAN may achieve a stealthy attack with a wider range of attack parameters. We also determine that natural phenomena with certain characteristics are more susceptible to the attack and require further sensing-verification mechanisms.**

***Index Terms*—Wireless Sensor-Actuator Networks (WSANs), Competing Networks, Sensing Attacks, Security**

I. Introduction

The unique characteristics and requirements of Wireless Sensor Networks (WSNs) have spurred much investigation into topics ranging from energy-efficient and distributed algorithms to security in the presence of captured or malicious nodes. In this rich pool of research we see a more recent interest in WSNs equipped with the ability to perform actuation on some phenomenon in the surrounding environment [1]. These networks of nodes are often referred to as Wireless Sensor Actuator (or Actor) Networks or WSAN for short. A WSAN may consist of a collection of low-energy limited-mobility WSN nodes with an additional set of higher-energy actuator (actor) nodes. In some cases a WSAN node may simply be an integrated robot-like unit that performs sensing, mobility and actuation.

This emerging WSAN paradigm is raising new questions about distributed coordination and cooperation between lower-energy WSN nodes and higher-energy actuator nodes [1]. Also largely unexplored are new questions regarding security and reliability in this new setting [2], [3]. One such new challenge stems from the possibility that actuation in an environment may affect the sensor readings registered by the WSN nodes, either accidentally or maliciously [4]. For instance we can envision a set of hostile actuator nodes that act upon a phenomenon of interest in their vicinity (for example by using micro-heaters). The aim of such actuation is to perturb or distort the sensor readings of other neighboring nodes within the actuation radius [4]. A possible scenario is shown in Fig. 1 where two networks (a WSN and a WSAN) belonging to different owners are deployed in a common environment. Each WSN node collects readings and makes a local decision about the presence or absence of a phenomenon of interest in the environment. These readings are eventually transmitted to the WSN's cluster head. The hostile WSAN network also collects readings and its very presence in the environment does not raise an initial alert. We note that both networks may possess actuation capabilities, however in this work we assume that only one of the networks (called the WSAN) employs actuation to disrupt the readings of the other network (called the WSN). Fig. 2 illustrates the situation where a WSAN node employs actuation to disrupt the readings of a neighboring WSN node, leading to a possibly erroneous decision [5].

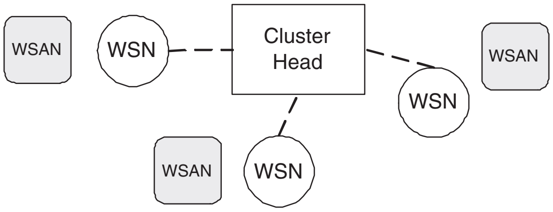

Fig. 1. Hostile WSAN nodes belonging to a foreign network are co-deployed with WSN nodes.

Since actuation affects sensing directly at the physical level of data collection, protection mechanisms relying on data encryption occur "too late" for the attack to be averted as shown in Fig. 3. The resulting loss in *sensing fidelity* (ie: reliability of data collected through sensing) has been referred to as a Denial of Service on Sensing (DoSS) in [4], [6]. In this work we wish to understand the probability that such an attack goes unnoticed at the cluster head. However the study of actuation attacks is complicated by considerations

1930-529X/07/$25.00 © 2007 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

of the specific *type* of sensor (i.e. temperature vs. pressure). Thus for generality and tractability reasons, in this work we do not consider the specific type of sensor but rather focus on the *effect* of an attack on a WSN *decision*. As shown in Fig. 3, we envision a WSN node that collects sensed readings and utilizes a local fixed threshold T_h to determine whether an event of interest has occurred in the environment. Incoming readings below T_h are mapped to a bit of value 0 and correspond to a WSN decision “event absent”. Conversely readings exceeding T_h are mapped to a bit of value 1 and correspond to the decision “event present”. Such decisions about the presence or absence of a phenomenon (event) of interest in the environment are envisioned for a variety of applications such as intelligent infrastructure monitoring [7]. In such an application, WSN nodes monitor a bridge for the presence of increased surface temperature and vibrations. When a given sensor threshold is exceeded, a decision (“event present”) is sent to the cluster head. The cluster head in turn activates selected wired cameras to begin recording the event. In all such applications, the sensing fidelity of the WSN nodes is of paramount importance.

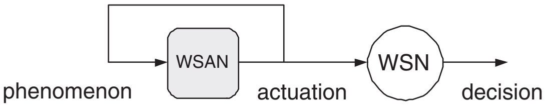

Fig. 2. Each WSAN node performs actuation upon its local phenomenon which affects both its own sensed readings as well as those of a neighboring WSN node.

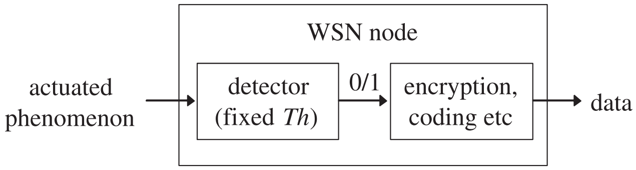

Fig. 3. Actuation occurs prior to internal signal processing or encryption. Here we depict our assumed model where a node maps its sensed readings to a 0 or 1 using a detector with a fixed threshold Th.

To enable attack detection in this challenging scenario, we assume that the cluster head of the WSN has access to information about the *average* count c (the number of nodes that report a 1). Such an average may be obtained from prior tests or abstract systems models and is largely application dependent. For instance, if the “event” of interest is the passing of a target through the WSN cluster, then based on the node deployment we may expect $c \pm \epsilon$ nodes in the cluster to witness the event. The cluster head however does not know *which* of the nodes will report a 1 (depending on the target’s trajectory). In general, given the average count c at the cluster head, the goal of the attacker is to affect the node decisions but in a *stealthy* way that avoids raising an alert. The resulting competitive *interaction* between the two networks may be viewed through a game theoretic perspective. We thus employ game theoretic analysis to understand the attack behavior of the hostile WSAN. We restrict our current analysis to a *single* play of the game (ie: a simultaneous-move, one-time game) though we note that the results generally hold for repeated games of infinite horizon (where the end time of the game is unknown to either network) [8].

To summarize, in this work we model and analyze the impact on sensing fidelity of a WSN in the presence of a *foreign hostile network* capable of actuation (ie: WSAN). To the best of our knowledge, this is the first attempt of its kind to analyze *two competing networks* in the context of sensing reliability and phenomenon-altering actuation (in contrast with studies of a single network with a few captured or misbehaving nodes that inject false packet data).

II. Related Work

Actuation in WSNs is an emerging topic with many open problems related to communication, coordination and security. In [1], Akyildiz and Kasimoglu present different types of WSAN networks including those consisting of a combination of lower-energy WSN nodes and higher-energy actor (actuator) nodes, or ones consisting of integrated devices. The authors present a comprehensive set of research challenges at various network layers associated with cooperation and coordination among the devices. In [5], Lin and Megerian study the problem of performing distributed actuation of controllable sources in large-scale WSANs where the sources are connected to actuators (such as in a lighting control application). They present a low-cost distributed algorithm which performs nearly as well as a centralized quadratic programming approach. Both of these papers provide key insights into control and coordination of sensor and actuator devices.

Security issues of WSANs are addressed by Hu *et al.* with specific emphasis on reliability and security of transmission among the sensor and actor nodes [2], [3]. The authors present a low-complexity transmission scheme based on local wireless hop repair, hop-to-hop retransmission and a two-level re-keying/re-routing scheme. As demonstrated in their work, WSAN security may not always borrow directly from WSN solutions due to special WSAN requirements. Similarly in [4], the authors examine the special security issues arising in WSANs due to actuation. The authors consider a form of actuation attack on sensed data based on a superposition model. Such a model assumes that actuation increases the intensity of the phenomenon sensed by the nodes in an additive way. In comparison, the model studied in this work does not assume a specific form for the actuation but instead examines a bit representation of the nodes’ data and focuses on the probability that these bits are altered by actuation.

The work of Ganeriwal and Srivastava focuses on WSN security but yields important insights for WSANs [9]. The authors consider attacks by malicious or misbehaving nodes within a *single* WSN and argue that cryptographic means alone are not sufficient to mitigate such attacks and suggest the use of statistics, data analysis and techniques from economics. Their proposed beta reputation system is based on a Bayesian

1930-529X/07/$25.00 © 2007 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

framework which allows nodes to evaluate and update the trustworthiness of other nodes. Similarly in [10], Felegyhazi *et al.* employ game theory (traditionally an economic toolset) to determine the conditions under which incentives are required in a WSN in order to achieve node cooperation (in the context of packet forwarding). Their analysis specifically accounts for the topology of the WSN and shows that for static WSN nodes, some incentives are required in practice.

III. System Model

We consider the presence of *two* competing wireless networks deployed in a common environment by *different* owners both of whom wish to collect their own data about (potentially different aspects of) some phenomenon in the environment. Both networks may possess actuation ability but we consider the case where only one of the networks is using actuation to cause a loss of sensing fidelity in the other network. For distinction purposes we refer to the actuation network as a WSAN that is "hostile" and to the second network as a WSN that is "legitimate" (non-hostile in its operation).

Fig. 1 depicts our assumed model where *each* WSAN node is in the vicinity of *one* WSN node for tractability purposes. In the absence of attack, we model the decision about the event of interest at a WSN node i by the random variable X_i. Based on our assumption of a binary decision (event present or absent), the probability distribution of X_i is modeled as a Bernoulli distribution such that $X_i \sim Bern(p)$ as given by Eq. 1. Thus the random vector $\mathbf{X} = (X_1, X_2, \ldots, X_n)$ models the output of the n sensor nodes in a cluster when no attack is present. We assume that the X_i are *i.i.d* within the cluster based on spatial deployment of the nodes.

$$X_i = \begin{cases} 1 & \text{w.p. } p \\ 0 & \text{w.p. } 1-p \end{cases} \tag{1}$$

The goal of each hostile WSAN node is to actuate (and hence alter) the decision reported by a WSN node in a stealthy way (so as to avoid alerting the WSN cluster head). Specifically, *each* hostile WSAN node i actuates according to a random variable Y_i where $y_i = 1$ indicates actuation and $y_i = 0$ indicates no actuation. The random variable Y_i is also modeled as Bernoulli with distribution $Y_i \sim Bern(q)$. The *effect* of an actuation is to "flip" the decision of a WSN node either from 1 to 0 or vice versa. Hence in our model the effect of actuation is given by $Z_i = X_i \oplus Y_i$, where X_i is the decision of a node i under no attack, Y_i is the attack and Z_i is the resulting decision that is reported to the cluster head. We note that although we started with the physical notion of an actuation attack, the resulting model is that of the familiar binary symmetric channel. We have thus translated a new unfamiliar problem into one that is well understood and which facilitates further analysis. We also note that ongoing work involves a stronger model of attack where coordination among the WSAN nodes in selecting y_i is permitted.

As mentioned in Section I and depicted in Fig. 3, actuation occurs directly at the physical level during sensing and *prior* to the protection afforded by mechanisms such as encryption. Furthermore, *each* WSN node has a probability q of being attacked. Such an attack may hence be quite challenging to detect under certain assumptions. In our model we assume that the cluster head of the WSN has information about an *average* count or weight $w_{avg}(\mathbf{x})$, such as from the spatial deployment, from prior averages or from an abstract system model. The count or weight $w(\mathbf{x})$ of a vector $\mathbf{x}$ is defined as $w(\mathbf{x}) = \sum_{i=1}^{n} x_i$. Importantly, the cluster head cannot know what specific weight to expect given that the phenomenon is random and the purpose of the WSN is to collect such data. The cluster head may merely use information about the average weight as an indicator of a possible sensing fidelity issue. For instance if the received weight deviates from $w_{avg}(\mathbf{x})$, say by more than some $\pm\epsilon$, the cluster head may initiate a secondary check to verify if the WSN is witnessing a rare event or if it is under attack. Given our previous assumption that $X_i \sim Bern(p)$, $w(\mathbf{X})$ is modeled by a binomial distribution, denoted $w(\mathbf{X}) \sim Binomial(n, p)$.

IV. Problem Formulation

The actuation scenario may be thought of as a game between the hostile WSAN and nature for control of the bits registered by the legitimate WSN nodes. In this game the WSN itself does not truly play any moves but merely collects the data and subjects it to verification at the cluster head. However it is sometimes convenient to think of this game conceptually as one between the WSAN and the WSN for control of the probability P_A of raising an alert (as will be defined). In this game the legitimate WSN "chooses" p to maximize the probability P_A of raising an alert if an attack is present, ie: $max_p\ P_A$. The hostile WSAN on the other hand chooses q so as to maximize the probability P_S of a successful stealthy attack, $max_q\ P_S$ or equivalently, $max_q\ (1 - P_A) = min_q\ P_A$. The goals of the two networks are hence conflicting and can be viewed as a zero-sum game with respect to P_A. We note that the overall objective of this formulation is to understand how the hostile WSAN should choose its q to alter the WSN's data while passing the alert test.

Based on the system model of Section III, the attack does not raise an alert at the cluster head if $|w(\mathbf{X} \oplus \mathbf{Y}) - w_{avg}(\mathbf{X})| < \epsilon$, or in other words, if the weight of the actuated phenomenon is within some $\pm\epsilon$ window centered around the *average* weight of the phenomenon (such as from prior statistics). This yields a probability P_S of stealthy attack success and a probability P_A of alert given by Eq. 2.

$$\begin{aligned} P_A &= 1 - P_S \\ &= 1 - Pr\{|w(\mathbf{X} \oplus \mathbf{Y}) - w_{avg}(\mathbf{X})| < \epsilon\} \\ &= Pr\{|w(\mathbf{X} \oplus \mathbf{Y}) - w_{avg}(\mathbf{X})| \geq \epsilon\} \end{aligned} \tag{2}$$

Importantly we note that the statistical alert test is not a true attack "detection" test but merely an alert to the *possibility* of tampering. Specifically, if the cluster head receives a weight that exceeds the $\pm\epsilon$ window, there is a possibility that it is witnessing an interesting rare natural occurrence. Conversely,

1930-529X/07/$25.00 © 2007 IEEE

with the right choice of attack parameter q, an attack may produce a weight within the $\pm\epsilon$ window and not raise an alert. The aim of this formulation hence is to determine how the choice of attack parameter q and the phenomenon parameter p ("chosen" by nature) affect the probability of raising an alert. The overall resulting game is summarized below.

Players	Player 1 (legitimate WSN)
	Player 2 (hostile WSAN)
Strategies	$S_1 = \{p : p \in [0,1]\}$
	$S_2 = \{q : q \in [0,1]\}$
Rules	Both players move at the same time.
	Neither player knows the strategy of the other.
Payoffs	$u_1(p,q) = -P_A$
	$u_2(p,q) = P_A$
Goal	Nash equilibria (pure strategies)

V. Results and Discussion

We begin by investigating a few properties of Eq. 2 for the case when $\epsilon = 0$, that is, we examine the conditions under which $w(\mathbf{x} \oplus \mathbf{y}) \;= w_{avg}(\mathbf{x})$. Let $k = w(\mathbf{x})$ be the weight of an unaffected data vector and let $l = w(\mathbf{y})$ be the weight of the actuation attack vector. It can be shown that $w(\mathbf{x} \oplus \mathbf{y}) = w_{avg}(\mathbf{x})$ *iff* the number of 1s in $\mathbf{x}$ and $\mathbf{y}$ coincide in exactly $m = \frac{w(\mathbf{y})}{2}$ positions. The key observation here is that coinciding bits of value 1 do not contribute to the weight of the resulting $w(\mathbf{x} \oplus \mathbf{y})$ based on modulo 2 addition. Furthermore it can be shown that given a number m and a pair (k,l), the relationships $n - w(\mathbf{x}) \geq w(\mathbf{y}) - m$, $n \geq k \geq m$ and $n \geq l \geq m$ must hold in order to avoid either k or l exceeding n, which is not admissible.

We can determine the conditional probability of $\mathbf{x}$ and $\mathbf{y}$ overlapping in exactly m positions, such as by using a technique that fixes one of the vectors, say $\mathbf{x}$, and then chooses $\mathbf{y}$s so that only m of their 1s overlap with any of the $\mathbf{x}$'s 1s. The total probability can then be obtained via summation over all possible k and l. The probability of such an event, which we denote by $P(E)$ is given by Eq. 3, where we have used binomial coefficients a, b and c defined below (where n, k, l and m are integers).

$$Pr(E) = \sum_{k=1}^{n}\sum_{l=1}^{n} a \cdot b \cdot c \cdot p^k(1-p)^{n-k}q^l(1-q)^{n-l} \quad (3)$$

$$\begin{aligned} a(k,m) &= \begin{cases} \binom{k}{m} & \text{if } k \geq m \\ 0 & \text{o.w} \end{cases} \\ b(k,l,m) &= \begin{cases} \binom{n-k}{l-m} & \text{if } n-k \geq l-m \\ 0 & \text{o.w} \end{cases} \\ c(k) &= \begin{cases} \binom{n}{k} & \text{if } n \geq k \\ 0 & \text{o.w} \end{cases} \end{aligned}$$

Combining Eq. 3 with the conditions required for $w(\mathbf{x} \oplus \mathbf{y}) = w_{avg}(\mathbf{x})$, we obtain the final result for the probability of attack success P_S (the probability that an attack does not trigger an alert at the cluster head):

$$\begin{aligned} P_S &= Pr\{|w(\mathbf{X} \oplus \mathbf{Y}) - w_{avg}(\mathbf{X})| < \epsilon\} \\ &= \sum_{m=\lceil \frac{l-\epsilon}{2} \rceil}^{\lfloor \frac{l+\epsilon}{2} \rfloor} \sum_{k=1}^{n}\sum_{l=1}^{n} a\,(k,m)\,b\,(k,l,m)\,c(k) \\ &\qquad \cdot p^k(1-p)^{n-k}q^l(1-q)^{n-l} \quad (4) \end{aligned}$$

For the game played between the two networks, the pure strategy Nash equilibria are the strategy vectors (p^*, q^*) where $(p^* \in [0,1],\ q^* \in [0,1])$ such that Player 1 would not find it beneficial to deviate from p^* given Player 2 plays q^*, and vice versa [8]. The game is difficult to solve in closed form for an arbitrary cluster size n. The function $P_S = Pr\{w(\mathbf{X} \oplus \mathbf{Y}) = w_{avg}(\mathbf{X})\} \doteq \psi(p,q)$ (ie: a function of both p and q) can be shown to be concave in p with peak at $p = \frac{1}{2}$ and semi-concave in q in the asymptotic case of large n. We now state a result for large n.

Theorem 1: Suppose that Player 1 can only play p^* from a closed subinterval of $[0,1]$, denoted $P = [a,b]$, $a < b$, while $q^* \in [0,1]$. For n sufficiently large, the pure strategy Nash equilibrium is given by:

$$p^* = \begin{cases} a & \text{if } a < |1-b| \\ b & \text{if } a > |1-b| \end{cases} \quad (5)$$

and $q^* = \delta$, where $\delta \downarrow 0$ as $n \to \infty$. If $a = |1-b|$, then there are two equilibria at (a,δ) and (b,δ).

In other words, the best hostile WSAN strategy for a *large* cluster is to keep q relatively *small*, though this may *not* be the case for smaller clusters as will be illustrated. Regarding the choice of p, if it can be chosen from the entire interval $[0,1]$, then the minima of $\psi(p)$ (ie: $\psi(p,q)$ with q treated as fixed) occur at $p^* = 0$ and $p^* = 1$. If instead we have to choose p from the closed subinterval $P \subset [0,1]$, then we would take either the left or right boundary of the subinterval, whichever is closer to 0 or 1 respectively. As stated earlier, p is not truly chosen by the legitimate WSN but rather represents the play by nature in producing the phenomenon. The analysis over the best "choice" of p is then really an analysis of the types of phenomena that are most resistant to the attack.

We now present some examples for realistic, finite sized networks in this WSN-WSAN game. We first examine a plot of $\varphi(q)$ (ie: $\psi(p,q)$ for fixed p), which corresponds to the probability of attack *success* P_S in the $\epsilon = 0$ case by the hostile WSAN. Figure 4(a) shows both the theoretical curve and a simulated curve (10^5 experiments). Based on Figure 4(a) for two networks each of size $n = 60$, and for a phenomenon of characteristic such that $p = 0.495$, the optimal q is $q^* \approx 0.05$, which is closer to 0 than to 0.5 and hence follows the trend stated by Theorem 1 for the asymptotic case. It can be seen that the highest probability of attack success in this case is actually 0.2, which is not very large but not negligible. Hence we see that in the example being considered, an actuation attack may successfully avoid raising an alert, though the probability of such an attack might be "acceptably small" for some applications. For other applications requiring high

1930-529X/07/$25.00 © 2007 IEEE

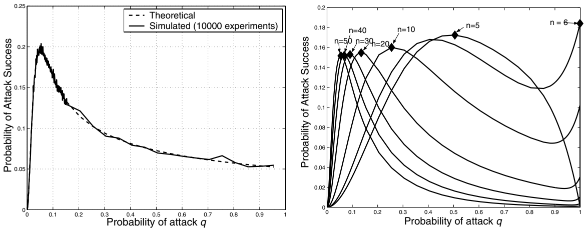

Fig. 4. (a)Theoretical vs. simulated $\varphi(q)$, probability of attack success, for $n = 60$ nodes, $p = 0.495$. (b) Probability of attack success, $\varphi(q)$, for $p = 0.3$ over various cluster sizes n.

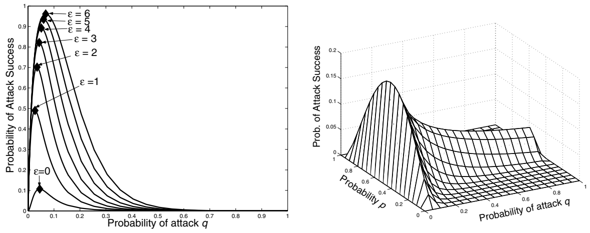

Fig. 5. (a) Probability of attack success, $\varphi(q)$, for $n = 55$ nodes, $p = 0.2$ over various ϵ uncertainty. (b) Probability of attack success, $\psi(p, q)$, manifold for $n = 60$ nodes and $p = 0.5$ (worst-case for WSN).

sensing fidelity, additional methods of detecting or preventing the attack are required. The actuation attack by a hostile WSAN is thus quite insidious, especially given that we have not assumed coordination among the WSAN nodes such that the attack vector $\mathbf{Y}$ is of a given weight.

Next we examine the effect of cluster size n on the optimal choice of q (i.e: q^*) which is shown in Figure 4(b). We note that as n becomes larger, the peak q^* approaches 0. Also interesting is the fact that for smaller n, there are usually two peaks, with the second peak closer to $q = 1$ indicating a high probability of attack. As n increases, this second peak starts to vanish giving the hostile WSAN only one option for avoiding detection, namely choosing a small q. We also see that as n increases, the *width* of the peak decreases giving the hostile WSAN less room for choosing a q that avoids detection. This result has implications for selecting an appropriate cluster size to minimize the chance of an undetected attack. It is also interesting to consider the effects of ϵ on the probability P_S of Eq. 2, as shown in Figure 5(a). The peak still occurs with q^* close to 0, but as ϵ increases, the height of the peak increases. This corresponds to the cluster head now admitting more varieties of strings as "natural" and hence the attacker having more "room" to hide the attack successfully. We note that the possible range of ϵ is application dependent (depending on the spatial deployment of nodes for example).

Finally we examine the overall $\psi(p, q)$ manifold for the two networks, each of size $n = 60$ and with ϵ set to 0 as shown in Figure 5(b). If Player 1 (legitimate WSN) can "choose" from the entire interval (recalling that the choice is actually made by nature), then Player 1 will choose $p = 0$ or $p = 1$ on the p-axis of Figure 5(b). Player 2 (hostile WSAN) on the other hand chooses a q that maximizes Figure 5(b). As we can see, any choice of q, given Player 1's $p = 0$ or $p = 1$ will result in an attack success probability of 0. This result confirms the fact that if the cluster head always expects $\mathbf{z} = \mathbf{0}$ (the all-zero vector) or $\mathbf{z} = \mathbf{1}$ (the all-one vector) for a fixed threshold at the detector, then no attack can fool the cluster head. On the other hand, phenomena that generate 1s and 0s with equal probability (ie: $p = 0.5$) given a fixed detector threshold are least "robust" to the attack.

VI. Conclusions and Future Extensions

In this work we model and assess the vulnerability of a WSN to an actuation attack carried out by a hostile WSAN. Since the actuation attack occurs *during* sensing (and hence prior to coding or encryption), we examine the case when the WSN has access to an average count or weight statistic to assist in checking the fidelity of the sensed data. We pose the problem as a game theory-based interaction between the WSN and the hostile WSAN for control of the probability of raising an alarm. To the best of our knowledge, the basic analysis presented here is the first of its kind to examine this emerging problem. Work in progress includes a coordinated attack by the WSAN relying on cooperation among the hostile nodes, and the study of other detection and prevention techniques such as limited mobility and the use of other statistical measures.

Acknowledgment

The authors would like to thank the reviewers for their insightful comments.

References

[1] I. Akyildiz and I. Kasimoglu, "Wireless sensor and actor networks: Research challenges," *Ad Hoc Networks Journal*, vol. 2, no. 4, pp. 3351–3677, 2004.

[2] F. Hu, X. Cao, S. Kumar, and K. Sankar, "Trustworthiness in wireless sensor and actuator networks: Towards low-complexity reliability and security," *IEEE GLOBECOM'05*, vol. 3, pp. 1696–1700, Nov 28- Dec 2 2005.

[3] F. Hu, N. Sheony, and X. Liu, "Robust security in large-scale wireless actuator and sensor networks: a low energy two-level implementation," *IEEE International Conference on Networking, Sensing and Control*, pp. 850–854, March 2005.

[4] A. Czarlinska and D. Kundur, "Distributed actuation attacks in wireless sensor networks: Implications and countermeasures," *Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, pp. 3–12, April 2006.

[5] Y.-T. Lin and S. Megerian, "Low cost distributed actuation in large-scale ad hoc sensor-actuator networks," *International Conference on Wireless Networks, Communications and Mobile Computing*, pp. 975–980, 2005.

[6] A. Czarlinska and D. Kundur, "Towards characterizing the effectiveness of random mobility against actuation attacks," *Journal of Computer Communications, Special Issue on Sensor Actuator Networks (SANETs), to appear*, 2007.

[7] A. Basharat, N. Catbas, and M. Shah, "A framework for intelligent sensor network with video camera for structural health monitoring of bridges," in *Proceedings. Third IEEE International Conference on Pervasive Computing And Communications Workshops, PerCom 2005 Workshops*, March 2005, pp. 385–9.

[8] M. J. Osborne, *An Introduction to Game Theory*. Oxford University Press, 2003.

[9] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks," *Security of Ad Hoc and Sensor Networks (SASN)*, pp. 66–77, Oct 25 2004.

[10] M. Felegyhazi, J.-P. Hubaux, and L. Buttyàn, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 5, pp. 463–476, 2006.